INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND PROGRAM STORAGE MEDIUM

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority from Japanese Application No. 2000-364897 filed November 30, 2000, the disclosure of which is hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

[0002] The present invention relates generally to an information processing apparatus, an information processing method and a program storage medium and, more particularly, to an information processing apparatus, an information processing method and a program storage medium for preventing unauthorized usage of content.

[0003] Various technologies are in use for preventing, on the basis of encryption, unauthorized usage of digital content of music and images, for example, from being practiced.

[0004] Referring to FIG. 1, there is shown a schematic diagram illustrating a related-art process of encrypting content for recording and decrypting the encrypted content for reproduction. An encryption program used in this example generates an encryption key on the basis of an input user ID and password and encrypts content by use of the generated encryption key.

[0005] To reproduce the encrypted content, a decryption program asks the user for his ID and password and, when the received ID and password are determined to be valid, generates a decryption key based thereon, and decrypts the encrypted content by use of the generated decryption key.

[0006] Thus, unless the correct ID and password are obtained, no user can access any content. Consequently, unauthorized usage of content can be prevented.

[0007] However, the above-mentioned unauthorized access prevention technology has a drawback. That is, if a malicious user publishes his ID and password, unauthorized third parties can access encrypted content with ease.

SUMMARY OF THE INVENTION

[0008] It is therefore an object of the present invention to provide an information processing apparatus, an information processing method and a program storage medium for preventing

any unauthorized third parties from accessing content.

[0009] In carrying out the invention and according to one aspect thereof, there is provided an information processing apparatus including a first receiver operable to receive settlement information for use in accounting settlement from another information processing apparatus; a data generator operable to generate identification data for identifying a user of content upon receipt of the settlement information, the identification data including the settlement information; and a transmitter operable to transmit the identification data to the another information processing apparatus.

[0010] The above-mentioned identification data is made up of an ID (Identification Data) and a password, one of the ID and the password including the settlement information.

[0011] The above-mentioned information processing apparatus may further include a recorder operable to record the identification data; a second receiver operable to receive the identification data; a comparing unit operable to compare the identification data recorded by the recorder with the identification data received by the second receiver to produce a comparison result; and a requesting unit operable to request a key providing apparatus to provide a key for decrypting the content to the another information processing apparatus based on the comparison result.

[0012] In carrying out the invention and according to another aspect thereof, there is provided a method for processing information in an information processing apparatus, including receiving settlement information for use in accounting settlement from another information processing apparatus; generating identification data for identifying a user of content upon receipt of the settlement information, the identification data including the settlement information; and transmitting the identification data to the another information processing apparatus.

[0013] In carrying out the invention and according to still another aspect thereof, there is provided a program storage medium storing a computer-readable program for processing information in an information processing apparatus, including receiving settlement information for use in accounting

settlement from another information processing apparatus; generating identification data for identifying a user of content upon receipt of the settlement information, the identification data including the settlement information; and transmitting the identification data to the another information processing apparatus.

[0014] In the information processing apparatus, the information processing method, and the program storage medium, settlement information for use in the settlement of fee charging is received from another information processing apparatus; upon reception of the settlement information, user identification data for identifying a user who uses digital content is generated, the identification data including the settlement information; and the generated user identification data is transmitted to the above-mentioned another information processing apparatus. Consequently, the novel constitution prevents authorized data from being spread unnecessarily, thereby preventing usage of the content by any unauthorized third parties.

[0015] In carrying out the invention and according to yet another aspect thereof, there is provided an information processing apparatus storing settlement information in correspondence with user identification data, including a first receiver operable to receive the settlement information from a first information processor; a decision unit operable to determine whether the received settlement information is recorded in the information processing apparatus; a data generator operable to generate the user identification data corresponding to the received settlement information if the received settlement information is not recorded in the information processing apparatus; a recorder operable to record the received settlement information in correspondence with the user identification data if the user identification data has been generated; a first transmitter operable to transmit the generated user identification data to the first information processor if the user identification data has been generated; a first retrieving unit operable to retrieve the user identification data recorded in correspondence with the settlement information if the received settlement information

is recorded in the information processing apparatus; and a second transmitter operable to transmit the retrieved user identification data to the first information processor if the user identification data has been read.

[0016] The above-mentioned information processing apparatus may further include a second receiver operable to receive the user identification data from a second information processor; a second retrieving unit operable to retrieve the settlement information recorded in correspondence with the user identification data received by the second receiver; and a third transmitter operable to transmit the retrieved settlement information to the second information processor.

[0017] The above-mentioned user identification data is used to identify a user who uses digital content.

[0018] In carrying out the invention and according to a different aspect thereof, there is provided a method for processing information in an information processing apparatus storing settlement information in correspondence with user identification data, including receiving the settlement information from another information processing apparatus; determining whether the received settlement information is recorded in the information processing apparatus; generating the user identification data corresponding to the received settlement information if the received settlement information is not recorded in the information processing apparatus; recording the received settlement information in correspondence with the user identification data if the user identification data has been generated; transmitting the generated user identification data to the another information processing apparatus if the user identification data has been generated; retrieving the user identification data recorded in correspondence with the settlement information if the received settlement information is recorded in the information processing apparatus; and transmitting the retrieved user identification data to the another information processing apparatus if the user identification data has been read.

[0019] In carrying out the invention and according to a still different aspect thereof, there is provided a program storage medium storing a computer-readable program for

processing information in an information processing apparatus storing settlement information in correspondence with user identification data, the computer-readable program including receiving the settlement information from another information processing apparatus; determining whether the received settlement information is recorded in the information processing apparatus; generating the user identification data corresponding to the received settlement information if the received settlement information is not recorded in the information processing apparatus; recording the received settlement information in correspondence with the user identification data if the user identification data has been generated; transmitting the generated user identification data to the another information processing apparatus if the user identification data has been generated; retrieving the user identification data recorded in correspondence with the settlement information if the received settlement information is recorded in the information processing apparatus; and transmitting the retrieved user identification data to the another information processing apparatus if the user identification data has been read.

[0020] In the information processing apparatus, the information processing method, and the program storage medium, settlement information is received from another information processing apparatus; a determination is made as to whether the received settlement information is already recorded in the information processing apparatus; user identification data corresponding to the settlement information is generated if the settlement information is not recorded in the information processing apparatus; the settlement information is recorded in correspondence with the generated user identification data; the user identification data is transmitted to the above-mentioned another information processing apparatus; and if the received settlement information is already recorded in the information processing apparatus, the user identification data recorded in correspondence with the settlement information is retrieved and transmitted to the above-mentioned another information processing apparatus. Consequently, the novel constitution prevents authorized data from being spread

unnecessarily, thereby preventing usage of the content by any unauthorized third parties.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] These and other objects of the invention will be seen by reference to the following description, taken in connection with the accompanying drawings, in which:

[0022] FIG. 1 is a schematic diagram illustrating a related-art software program for encrypting content for recording and decrypting the encrypted content for reproduction;

[0023] FIG. 2 is a block diagram illustrating a music data management system practiced as one embodiment of the invention;

[0024] FIG. 3 is a block diagram illustrating an exemplary configuration of a personal computer;

[0025] FIG. 4 is a block diagram illustrating an exemplary configuration of an approval server;

[0026] FIG. 5 is a block diagram illustrating an exemplary functional configuration of the personal computer;

[0027] FIG. 6 is a schematic diagram illustrating content stored in a personal computer;

[0028] FIG. 7 is a schematic diagram illustrating content to be output from the personal computer;

[0029] FIG. 8 is a schematic diagram illustrating an operation by a personal computer which imports content;

[0030] FIG. 9 is a schematic diagram illustrating an approval operation by the approval server when importing content;

[0031] FIG. 10 is a schematic diagram illustrating a process for registering personal computers belonging to one group with the approval server;

[0032] FIG. 11 is a schematic diagram illustrating a process for importing content;

[0033] FIG. 12 is a flowchart describing the registration process;

[0034] FIG. 13 is a flowchart describing one example of generating a group ID and password;

[0035] FIG. 14 is a flowchart describing outputting of content;

[0036] FIG. 15 is a flowchart describing importing of content;

[0037] FIG. 16 is a schematic diagram illustrating another example of managing a group ID and password;

[0038] FIG. 17 is a flowchart describing a registration process;

[0039] FIG. 18 is a flowchart describing the process of generating an ID and password by an ID management server;

[0040] FIG. 19 is a flowchart describing a registration process by the personal computer and an EMD server;

[0041] FIG. 20 is a flowchart describing accounting settlement processing;

[0042] FIG. 21 is a schematic diagram illustrating another processing operation of importing content;

[0043] FIG. 22 is a flowchart describing the process of transmitting a group key;

[0044] FIG. 23 is a schematic diagram illustrating the process of registration with a locker server;

[0045] FIG. 24 illustrates one example of a list of content stored in the locker server;

[0046] FIG. 25 is a schematic diagram illustrating one example of the shared use of content supported by the locker server;

[0047] FIG. 26 is a schematic diagram illustrating another example of the shared use of content supported by the locker server;

[0048] FIG. 27 is a schematic diagram illustrating fee-charging processing by the locker server;

[0049] FIG. 28 is a flowchart describing registration processing by the personal computer and the locker server;

[0050] FIG. 29 is a flowchart describing the process of recording content to the locker server;

[0051] FIG. 30 is a flowchart describing the process of reading content from the locker server;

[0052] FIG. 31 is a schematic diagram illustrating a music data management system practiced as a second embodiment of the invention;

[0053] FIG. 32 is a perspective view of a camera-mounted digital mobile telephone;

[0054] FIG. 33 is a partial perspective view of the camera-mounted digital mobile telephone; and

[0055] FIG. 34 is a block diagram illustrating an exemplary configuration of the camera-mounted digital mobile telephone.

DETAILED DESCRIPTION

[0056] This invention will be described in further detail by way of example with reference to the accompanying drawings. Now, referring to FIG. 2, there is shown one preferred embodiment of a music data management system associated with the present invention. As shown, a personal computer 1-1 is connected to a network 2 which is a local area network or the Internet, for example.

[0057] The personal computer 1-1 executes a content management program 51, a display operation instruction program 52, and purchase application programs 54-1 through 54-3 and, at the same time, internally constitutes a content database 53.

[0058] The content management program 51 encrypts content and stores the encrypted content in the content database 53 and manages the use of the content stored in the content database 53, which will be detailed later.

[0059] The display operation instruction program 52 displays content-associated information and, at the same time, instructs the content management program 51 to reproduce or import content or execute other inputs made by the user.

[0060] The content database 53 stores the content encrypted and supplied from the content management program 51 and, upon request from the content management program 51, supplies the encrypted content thereto.

[0061] The purchase application programs 54-1 through 54-3 execute the process of purchasing content from EMD servers 4-1 through 4-3. The purchase application programs 54-1 through 54-3 are connected to the content management program 51 via SAC (Secure Authentication Channel).

[0062] The purchase application program 54-3 executes a group gateway program 61. The group gateway program 61, when outputting encrypted content, encrypts a content key for decrypting the encrypted content by a group key, to be described later, to allow the use of the content only on authorized equipment. The group gateway program 61, when

importing encrypted content, decrypts the content key for decrypting the encrypted content by a group key to be described later. "Import" herein denotes the recording of content in a usable state.

[0063] The personal computer 1-1 and the personal computer 1-2 send the number of the credit card of the user to an approval server 3 via the network 2 for registration with the approval server 3, thereby acquiring a group key, and ID, and a password from the approval server 3, which will be described later.

[0064] The approval server 3, when the personal computer 1-1 has been registered, records the credit card number, ID, and password of the user of the personal computer 1-1 to an ID management server 8. The approval server 3 approves the personal computer 1-2 when the personal computer 1-2 imports content output from the personal computer 1-1, for example.

[0065] The personal computer 1-2, when not approved by the approval server 3, cannot import content output from the personal computer 1-1.

[0066] The personal computer 1-1 compresses music data (hereafter referred to as content) received from EMD (Electrical Music Distribution) servers 4-1 through 4-3 or read from a CD (Compact Disc) to be described later in a predetermined compression algorithm, ATRAC3 (trademark) for example, and encrypts the compressed content in a predetermined encryption algorithm such as DES (Data Encryption Standard), storing the resultant content.

[0067] The personal computer 1-1 records usage rule data for the encrypted and recorded content. The usage rule data includes conditions that the content matching the usage rule data can be used or copied on three portable devices (also referred to as PDs) 12-1 through 12-3 at a time, moved to other personal computers, and so on, for example.

[0068] The personal computer 1-1 stores the encrypted and recorded content in the connected portable device 12-1 along with content-associated data (for example, music title, the number of reproduction times, expiration of reproduction, equalizer information, and so on) and updates the usage rule data corresponding to this stored content (this updating is

hereafter referred to also as checkout). The personal computer 1-1 stores the encrypted and recorded content in the connected portable device 12-2 along with content-associated data and accordingly updates the usage rule data corresponding to this stored content. The personal computer 1-1 stores the encrypted and recorded content in the connected portable device 12-3 along with content-associated data and accordingly updates the usage rule data corresponding to this stored content.

[0069] Also, the personal computer 1-1 causes the connected portable device 12-1 to delete the content checked out by the personal computer 1-1 and accordingly updates the usage rule data corresponding to the deleted content (this updating is hereafter referred to also as check-in). The personal computer 1-1 causes the connected portable device 12-2 to delete the content checked out by the personal computer 1-1 and accordingly updates the usage rule data corresponding to the deleted content. The personal computer 1-1 causes the connected portable device 12-3 to delete the content checked out by the personal computer 1-1 and accordingly updates the usage rule data corresponding to the deleted content.

[0070] The personal computer 1-1 cannot check in the content checked out by the personal computer 1-2 to the portable device 12-1. The personal computer 1-1 cannot check in the content checked out by the personal computer 1-2 to the portable device 12-2. The personal computer 1-1 cannot check in the content checked out by the personal computer 1-2 to the portable device 12-3.

[0071] The personal computer 1-2 is connected to the network 2, which is a local area network or the Internet. The personal computer 1-2 compresses the content received from the EMD servers 4-1 through 4-3 or read from a CD to be described later in a predetermined algorithm and encrypts the compressed content in a predetermined algorithm such as DES, storing the resultant content in personal computer 1-2.

[0072] The personal computer 1-2 records usage rule data for the encrypted and recorded content. The usage rule data includes rules that the content matching the usage rule data can be used or copied on three portable devices at a time, moved to other personal computers, and so on, for example.

[0073] The personal computer 1-2 stores the encrypted and recorded content in the connected portable device 12-4 along with content-associated data and updates the usage rule data corresponding to this stored content (namely, checkout). When content checkout is instructed, the personal computer 1-2 will not check the content to the portable device 12-4 if a usage time limit or a permitted reproduction count to be described later is set to that content.

[0074] Also, the personal computer 1-2 causes the connected portable device 12-4 to delete the content checked out by the personal computer 1-2 and accordingly updates the usage rule data corresponding to the deleted content.

[0075] The personal computer 1-2 cannot check in the content checked out by the personal computer 1-1 to the portable device 12-4.

[0076] In what follows, the personal computers 1-1 and 1-2 are generically referred to as a personal computer 1 unless otherwise noted.

[0077] The EMD server 4-1, in response to a request from the personal computer 1, supplies content thereto along with content-associated data via the network 2. The EMD server 4-2, in response to a request from the personal computer 1, also supplies content thereto along with content-associated data via the network 2.

[0078] The EMD server 4-3, in response to a request from the personal computer 1, supplies the content supplied from the EMD content database 5 or an uploaded content database 6 to the personal computer 1 along with content-associated data (for example, music title, the number of reproduction times, expiration of reproduction, equalizer information, and so on), via the network 2. The EMD server 4-3 supplies the advertisement data supplied from an advertisement system 7 to the personal computer 1-1 or 1-2 via the network 2.

[0079] The content to be supplied by the EMD servers 4-1 through 4-3 is compressed by the same or different compression algorithms. The content to be supplied by the EMD servers 4-1 through 4-3 is encrypted by the same or different encryption algorithms.

[0080] When the user purchases content from any of the EMD

servers 4-1 through 4-5, the ID management server 8 sends the credit card number, ID, and password of the user of the personal computer 1-1 recorded upon registration thereof to any of the EMD servers 4-1 through 4-5 from which the content is to be purchased. When the content is purchased, the EMD servers 4-1 through 4-5 execute a fee-charging process on the basis of the credit card number, ID, and password supplied from the ID management server 8.

[0081] The group manager system 9 manages content, ID, and password usage rules such as the registration of the approval server 3, the approval of content usage, and recording and transmission of credit card numbers, IDs, and passwords by the ID management server 8.

[0082] A locker server 11 records the content supplied from the personal computer 1-1 or 1-2 via the network 2 and, in response to a request to send content, transmits the recorded content to the personal computer 1-1 or 1-2.

[0083] The portable device 12-1 stores the content supplied from the personal computer 1 (namely, the checked out content) in a loaded memory card 13-1 along with the content-associated data (for example, music title, the number of reproduction times, expiration of reproduction, equalizer information, and so on). The portable device 12-1 reproduces the content from the memory card 13-1 on the basis of the content-associated data and outputs the reproduced content to a headphone, not shown, for example.

[0084] For example, if the user attempts to reproduce the content in excess of the number of times the content is allowed to be reproduced, which is recorded as content-associated data, the portable device 12-1 disables the reproduction of this content. If the user attempts to reproduce the content after the expiration of reproduction, which is recorded as content-associated data, the portable device 12-1 disables the reproduction of this content. The portable device 12-1 equalizes an audio signal on the basis of the equalizer information recorded as content-associated data and outputs the equalized audio signal.

[0085] The user can unload the portable device 12-1 from the personal computer 1, carry about the portable device 12-1,

reproduce the content stored in the memory card 13-1, and, for example, listen to the music corresponding to the content through a headphone.

[0086] The portable device 12-1 can reproduce the content stored in the memory card 13-2 by loading the same into the portable device 12-1, the content being supplied from a terminal device 14 installed in a store, for example.

[0087] The memory card 13-1 in which content is stored via the portable device 12-1 is unloaded therefrom and loaded in an audio set of an automobile 15. The audio set of the automobile 15 with the memory card 13-1 loaded therein retrieves the content from the memory card 13-1 and reproduces the retrieved content.

[0088] A camera-mounted digital mobile telephone 16 with the memory card 13-3 loaded therein asks the EMD server 4-4 for the supply of content via the network 2 and stores the supplied content into the memory card 13-3. The camera-mounted digital mobile telephone 16 reproduces the content stored in the loaded memory card 13-3. The portable device 12-1 can reproduce the content stored in the memory card 13-3 by loading the same into the portable device 12-1.

[0089] The portable device 12-2 stores the content supplied from the personal computer 1 along with the content-associated data. On the basis of the content-associated data, the portable device 12-2 reproduces the stored content and outputs the reproduced content to a headphone, not shown, for example. The user can unload the portable device 12-2 storing the content from the personal computer 1, carry about the portable device 12-2, reproduce the stored content, and listen to the music corresponding to the content through the headphone, for example.

[0090] The portable device 12-3 stores the content supplied from the personal computer 1 along with the content-associated data. On the basis of the content-associated data, the portable device 12-3 reproduces the stored content and outputs the reproduced content to a headphone, not shown, for example. The user can unload the portable device 12-3 storing the content from the personal computer 1, carry about the portable device 12-3, reproduce the stored content, and listen to the

music corresponding to the content through the headphone, for example.

[0091] The portable device 12-4 stores the content (only the content to which usage expiration or the number of reproduction times to be described later are not set) supplied from the personal computer 1 along with the content-associated data. On the basis of the content-associated data, the portable device 12-4 reproduces the stored content and outputs the reproduced content to a headphone, not shown, for example. The user can unload the portable device 12-4 storing the content from the personal computer 1, carry about the portable device 12-4, reproduce the stored content, and listen to the music corresponding to the content through the headphone, for example.

[0092] A home audio set 17 asks the EMD server 4-5 for content via the network 2, stores the requested content supplied from the EMD server 4-5, and reproduces the stored content.

[0093] Referring to FIG. 3, there is shown an exemplary configuration of the personal computer 1-1. A CPU (Central Processing Unit) 71 actually executes various application programs such as the content management program 51 and a group gateway program 61, and an OS (Operating System). A ROM (Read Only Memory) 72 generally stores computer programs and basically fixed data of computational parameters to be used by the CPU 71. A RAM 73 stores computer programs to be used by the CPU 71 in its execution and parameters which change from time to time in the execution. The CPU 71, ROM 72, and RAM 73 are connected each other by host bus 74 constituted by a CPU bus, etc.

[0094] The host bus 74 is connected to an external bus 76 such as a PCI (Peripheral Component Interconnect/Interface) via a bridge 75.

[0095] A keyboard 78 is operated by the user to enter various commands into the CPU 71. A mouse 79 is operated by the user to specify or select points on the screen of a display 80 which is constituted by a liquid crystal display, a CRT (Cathode Ray Tube), and the like. The CRT display 80 displays various kinds of information in text and images. An

HDD (Hard Disk Drive) 81 drives a hard disk to record or reproduce programs to be executed by the CPU 71 or information.

[0096] A drive 82 reads data or computer programs from a magnetic disc 91, an optical disc 92 (including a CD), a magneto-optical disc 93, or a semiconductor memory 94 as required to supply the data or computer programs to the RAM 73 via the interface 77, the external bus 76, the bridge 75, and the host bus 74.

[0097] USB (Universal Serial Bus) port 83-1 is connected to the portable device 12-1 through a predetermined cable. The USB port 83-1 outputs the data (including content or a command of the portable device 12-1, for example) supplied from the HDD 81, the CPU 71, or the RAM 73 to the portable device 12-1 via the interface 77, the external bus 76, the bridge 75, and the host bus 74.

[0098] The USB 83-2 is connected to the portable device 12-2 through a predetermined cable. The USB port 83-2 outputs the data (including content or a command of the portable device 12-2, for example) supplied from the HDD 81, the CPU 71, or the RAM 73 to the portable device 12-2 via the interface 77, the external bus 76, the bridge 75, and the host bus 74.

[0099] The USB 83-3 is connected to the portable device 12-3 through a predetermined cable. The USB port 83-3 outputs the data (including content or a command of the portable device 12-3, for example) supplied from the HDD 81, the CPU 71, or the RAM 73 to the portable device 12-3 via the interface 77, the external bus 76, the bridge 75, and the host bus 74.

[0100] A speaker 84 outputs a predetermined audio signal corresponding to the content on the basis of the data or audio signal supplied from the interface 77.

[0101] These components, the keyboard 78 through the speaker 84, are connected to the interface 77 which is connected to the CPU 71 via the external bus 76, the bridge 75, and the host bus 74.

[0102] A communication block 85 connected to the network 2 transmits, in predetermined packets, the data (for example, a registration request or a content send request) supplied from the CPU 71 or the HDD 81, and outputs the data (for example, authentication key and content) contained in received packets

to the CPU 71, the RAM 73, or the HDD 81, via the network 2.

[0103] The communication block 85 is also connected to the CPU 71 via the external bus 76, the bridge 75, and the host bus 74.

[0104] The configuration of the personal computer 1-2 is the same as that of the personal computer 1-1, so that its description will be skipped.

[0105] Referring to FIG. 4, there is shown an exemplary configuration of the approval server 3. A CPU 101 actually executes various application programs such as a Web server program and an OS. A ROM 102 generally stores computer programs and basically fixed data of computational parameters to be used by the CPU 101. A RAM 103 stores computer programs to be used by the CPU 101 in its execution and parameters which change from time to time in the execution. The CPU 101, ROM 102, and RAM 103 are connected each other by a host bus 104 constituted by a CPU bus, for example.

[0106] The host bus 104 is connected to an external bus 106 such as a PCI via a bridge 105.

[0107] A keyboard 108 is operated by the user to enter various commands into the CPU 101. A mouse 109 is operated by the user to specify or select points on the screen of a display 110 which is constituted by a liquid crystal apparatus, a CRT, and the like. The display 110 displays various kinds of information in text and images. An HDD 111 drives a hard disk to record or reproduce programs to be executed by the CPU 101 or information.

[0108] A drive 112 reads data or computer programs from a magnetic disc 131, an optical disc 132, a magneto-optical disc 133, or a semiconductor memory 134 as required to supply the data or computer programs to the RAM 103 via the interface 107, the external bus 106, the bridge 105, and the host bus 104.

[0109] These components, the keyboard 108 through the drive 112, are connected to the interface 107 which is connected to the CPU 101 via the external bus 106, the bridge 105, and the host bus 104.

[0110] A communication block 113, connected to the network 2, outputs the data (for example, the data necessary for registration to be described later, or the ID (Identifier) of

a predetermined program) stored in the received packets to the CPU 101, the RAM 103, or the HDD 111 and stores the data (for example, ID and password) supplied from the CPU 101 or the HDD 111 into predetermined packets to send them through the network 2.

[0111] The communication block 113 is connected to the CPU 101 via the external bus 106, the bridge 105, and the host bus 104.

[0112] The configuration of each of the EMD servers 4-1 through 4-5, the ID management server 8, and the locker server 11 is the same as that of the approval server 3, so that their description will be skipped.

[0113] The following describes the features which will be realized by the personal computer 1-1 by executing predetermined programs.

[0114] Referring to FIG. 5, there is shown a block diagram illustrating the features of the personal computer 1-1 which are realized by the execution of predetermined programs by the CPU 71.

[0115] The content management program 51 is made up of a plurality of programs including an EMD select program 171, a check-in/checkout management program 172, an encryption scheme conversion program 173, a compression scheme conversion program 174, an encryption program 175, a usage rule conversion program 176, a signature management program 177, an authentication program 178, a decryption program 179, and a PD driver 180.

[0116] The content management program 51, written by shuffled instructions or encrypted instructions, is constituted to hide the content of its processing from the outside, making it difficult to interpret the processing content (for example, if the user directly reads the content management program 51, no instruction can be identified).

[0117] The EMD select program 171, when the content management program 51 is installed on the personal computer 1, is not included therein, but is supplied from a registration server, not shown, via the network 2 when EMD registration is performed. The EMD select program 171 selects the connection with any one of the EMD servers 4-1 through 4-3 and causes the

purchase application programs 54-1 through 54-3 to execute the communication (for example, downloading of content at the time of content purchase) with any one of the EMD servers 4-1 through 4-3.

[0118] The check-in/checkout management program 172 sets check-in or checkout, checks out the content stored in content files 201-1 through 201-N to any one of the portable devices 12-1 through 12-3 on the basis of usage rule files 202-1 through 202-N recorded in the content database 53, or checks in the content stored in the portable devices 12-1 through 12-3.

[0119] The check-in/checkout management program 172 updates the usage rule data stored in the usage rule files 202-1 through 202-N recorded in the content database 53 in accordance with the process of check-in or checkout.

[0120] The encryption scheme conversion program 173 converts the encryption scheme of the content received by the purchase application program 54-1 from the EMD server 4-1 via the network, the encryption scheme of the content received by the purchase application program 54-2 from the EMD server 4-2 via the network, or the encryption scheme of the content received by the purchase application program 54-3 from the EMD server 4-3 via the network into the encryption scheme of the content stored in the content files 201-1 through 201-N recorded in the content database 53.

[0121] Also, when checking out content to the portable device 12-1 or 12-3, the encryption scheme conversion program 173 converts the encryption scheme of the content to be checked out into that usable by the portable device 12-1 or the 12-3.

[0122] The compression scheme conversion program 174 converts the compression scheme of the content received by the purchase application program 54-1 from the EMD server 4-1 via the network 2, the compression scheme of the content received by the purchase application program 54-2 from the EMD server 4-2 via the network 2, or the compression scheme of the content received by the purchase application program 54-3 from the EMD server 4-3 via the network 2 into the compression scheme of the content stored in the content files 201-1

through 201-N recorded in the content database 53.

[0123] The compression scheme conversion program 174 encodes the content (not compressed) read from a CD for example and supplied from a recording program 151 in the same encoding algorithm as that used on the content stored in the content files 201-1 through 201-N recorded in the content database 53.

[0124] Also, when checking out content to the portable device 12-1 or 12-3, the compression scheme conversion program 174 converts the compression scheme of the content to be checked out into the compression scheme usable on the portable device 12-1 or 12-3.

[0125] The encryption program 175 encrypts the content (not encrypted) read from a CD for example and supplied from the recording program 151 in the same encryption scheme as that used on the content stored in the content files 201-1 through 201-N recorded in the content database 53.

[0126] The usage rule conversion program 176 converts the format of the data indicative of the usage rules of the content received by the purchase application program 54-1 from the EMD server 4-1 via the network 2, the data indicative of the usage rules of the content received by the purchase application program 54-2 from the EMD server 4-2 via the network 2, or the data indicative of the usage rules of the content received by the purchase application program 54-3 from the EMD server 4-3 via the network 2 into the same format as that of the usage rule data stored in the usage rule files 202-1 through 202-N recorded in the content database 53.

[0127] Also, when checking out content to the portable device 12-1 or 12-3, the usage rule conversion program 176 converts the usage rule data corresponding to the content to be checked out into the usage rule data usable on the portable device 12-1 or 12-3.

[0128] The signature management program 177 checks, before performing check-in or checkout processing, the usage rule data for any alteration on the basis of the signature included in the usage rule data stored in the usage rule files 202-1 through 202-N recorded in the content database 53. The signature management program 177 updates the signature

included in the usage rule data in response to the updating of the usage rule data stored in the usage rule files 202-1 through 202-N recorded in the content database 53 which is executed at the time of check-in or checkout processing.

[0129] The authentication program 178 executes cross authentication between the content management program 51 and the purchase application program 54-1, the content management program 51 and the purchase application program 54-2, and the content management program 51 and the purchase application program 54-3. Also, the authentication program 178 stores authentication keys for use in executing cross-authentication between the EMD server 4-1 and the purchase application program 54-1, the EMD server 4-2 and the purchase application program 54-2, and the EMD server 4-3 and the purchase application program 54-3.

[0130] The authentication key for use by the cross-authentication by the authentication program 178 is not stored in the authentication program 178 when the content management program 51 is installed in the personal computer 1. When the registration process has been normally performed by the display operation instruction program 52, the authentication key is supplied from a registration server, not shown, to be stored in the authentication program 178.

[0131] The decryption program 179 decrypts content when the personal computer 1-1 reproduces the content stored in the content files 201-1 through 201-N recorded in the content database 53.

[0132] When checking out predetermined content to the portable device 12-2 or checking in predetermined content therefrom, the PD driver 180 supplies commands for causing the portable device 12-2 to execute the content or predetermined processing.

[0133] When checking out predetermined content to the portable device 12-1 or checking in predetermined content therefrom, the PD driver 180 supplies commands for causing the device driver 152-1 to execute the content or predetermined processing.

[0134] When checking out predetermined content to the portable device 12-3 or checking in predetermined content

therefrom, the PD driver 180 supplies commands for causing the device driver 152-2 to execute the content or predetermined processing.

[0135] The display operation instruction program 52 displays a predetermined window image on the display 80 on the basis of a filtering data file 221, a display data file 222, image files 223-1 through 223-K, or a log data file 224 and instructs the content management program 51 to execute check-in or checkout processing in response to an operation made by the user on the keyboard 78 or the mouse 79.

[0136] The filtering data file 221 stores the data for weighting each content stored in the content files 201-1 through 201-N recorded in the content database 53 and is stored in the HDD 81.

[0137] The display data file 222 stores the data about the content stored in the content files 201-1 through 201-N recorded in the content database 53 and is stored in the HDD 81.

[0138] The image files 223-1 through 223-K store the images for the content files 201-1 through 201-N stored in the content database 53 or the images for a package and are stored in the HDD 81.

[0139] The log data file 224 stores the log data such as the number of times the content stored in the content files 201-1 through 201-N recorded in the content database 53 has been checked out and checked in and the dates of checkout and check-in, and the log data file 224 is stored in the HDD 81.

[0140] At the time of registration processing, the display operation instruction program 52 transmits, via the network 2, the ID of the content management program 51 which is stored beforehand to a registration server, not shown, and, at the same time, receives an authentication key and the EMD select program 171 from the registration server to supply them to the content management program 51.

[0141] When recording is instructed, the recording program 151 reads content from the CD, which is the optical disk 92 loaded in the drive 82, and outputs the content to the content management program 51 along with the content-associated usage rule data such as the maximum number of permitted checkouts.

[0142] The content database 53 stores the content compressed in a predetermined compression scheme and encrypted in a predetermined encryption scheme supplied from the content management program 51 into one of the content files 201-1 through 201-N (recorded in the HDD 81). The content database 53 stores the usage rule data for the content stored in the content files 201-1 through 201-N in one of the usage rule files 202-1 through 202-N (recorded in the HDD 81) corresponding to the content files 201-1 through 201-N in which the content is stored.

[0143] The content database 53 may record the content files 201-1 through 201-N or the usage rule files 202-1 through 202-N as records.

[0144] For example, the usage rule data for the content stored in the content file 201-1 are stored in the usage rule file 202-1. The usage rule data for the content stored in the content file 201-N are stored in the usage rule file 202-N.

[0145] A startup program 153 is a so-called resident program which is always operating when the operating system of the personal computer 1-1 is active. When a signal comes from the device driver 152-1 telling that the portable device 12-1 has been connected to the USB port 83-1, the startup program 153 starts the display operation instruction program 52 if the program 52 is not activated.

[0146] When a signal comes from the device driver 152-2 telling that the portable device 12-3 has been connected to the USB port 83-3, the startup program 153 starts the display operation instruction program 52 if the program 52 is not activated.

[0147] In what follows, the content files 201-1 through 201-N will be generically referred to simply as a content file 201 unless otherwise noted. Likewise, the usage rule files 202-1 through 202-N will be generically referred to simply as a usage rule file 202 unless otherwise noted.

[0148] The functional configuration of the personal computer 1-2 is the same as that of the personal computer 1-1, so that its description will be skipped.

[0149] In what follows, the personal computer 1-1 and the personal computer 1-2 will be generically referred to simply

as a personal computer 1 unless otherwise noted.

[0150] Referring to FIG. 6, there is shown a schematic diagram illustrating content stored in the personal computer 1. The purchase application program 54-1 receives content encrypted by a content key from the EMD server 4-1 along with this content key and supplies the received content to the content management program 51 via the SAC. The purchase application program 54-1 decrypts the content key encrypted by a session key, for example, and supplies the decrypted content key to the content management program 51.

[0151] The purchase application program 54-2 receives content encrypted by a content key from the EMD server 4-2 along with this content key and supplies the received content to the content management program 51 via the SAC. The purchase application program 54-2 decrypts the content key encrypted by a session key, for example, and supplies the decrypted content key to the content management program 51.

[0152] The purchase application program 54-3 receives content encrypted by a content key from the EMD server 4-3 along with this content key and supplies the received content to the content management program 51 via the SAC. The purchase application program 54-3 decrypts the content key encrypted by a session key, for example, and supplies the decrypted content key to the content management program 51.

[0153] At the time of registration with the approval server 3, the group gateway program 61 transmits the credit card number and ID of the content management program 51 which are stored beforehand to the approval server 3 and receives the group key, ID, and password from the approval server 3.

[0154] The content management program 51 stores a storage key 253 beforehand and, upon request from the display operation instruction program 52, encrypts, by this storage key 253, the content key supplied from the purchase application program 54-1, the content key supplied from the purchase application program 54-2, or the content key supplied from the purchase application program 54-3.

[0155] The content management program 51 records content 251 encrypted by the content key and a content key 252 encrypted by the storage key 253 in the content database 53 as

the content file 201.

[0156] Referring to FIG. 7, there is shown a schematic diagram illustrating content to be output by the personal computer 1. The group gateway program 61 of the purchase application program 54-3 asks the content management program 51 for content 251-1.

[0157] The content management program 51 reads the content 251-1 and the content key 252 from the content database 53. The content management program 51 decrypts the content key 252 by the storage key 253 and supplies the decrypted content key to the group gateway program 61 along with the content 251-1 encrypted by the content key.

[0158] The group gateway program 61 encrypts the decrypted content key by a group key 271 and outputs content 251-2 encrypted by the content key along with content key 272 encrypted by the group key 271.

[0159] The content 251-2 output from the personal computer 1 is encrypted by the content key 272 and the content key 272 is encrypted by the group key 271, so that the content 251-2 cannot be used as it is.

[0160] The following describes an operation of the personal computer 1-2 which imports the content 251-2 from the personal computer 1-1 with reference to FIG. 8.

[0161] When the correct ID and password have been input and an approval is obtained from the approval server 3, a group gateway program 61-2 of the personal computer 1-2 decrypts the content key 272 by a group key 271-2 stored beforehand.

[0162] The group key 271-2 stored in the group gateway program 61-2 is the same as the group key 271-1 stored in the group gateway program 61-1.

[0163] The group gateway program 61-2 supplies the decrypted content key and the content 251-2 encrypted by this content key to the content management program 51-2.

[0164] The content management program 51-2 encrypts the content key by a storage key 253-2 and records content 251-3 encrypted by the content key into a content database 53-2 along with the content key 252-2 encrypted by the storage key 253-2.

[0165] When using the content 251-3 imported from the

personal computer 1-1, the personal computer 1-2 decrypts the content key 252-2 by the storage key 51-2 and decrypts the content 251-3 by the decrypted content key to provide plaintext content.

[0166] Thus, the personal computer 1-1 and the personal computer 1-2, respectively having the group key 271-1 and the group key 271-2 having a same value, are regarded as belonging to a same group.

[0167] The group key 271-1 and the group key 271-2 having a same value are supplied from the approval server 3 at the time of registration.

[0168] As shown in FIG. 9, the personal computer 1-2 belonging to the same group to which the personal computer 1-1 belongs can import content output from the personal computer 1-1 when approved by the approval server 3.

[0169] However, a personal computer 281 which does not belong to the same group to which the personal computer 1-1 belongs cannot import and use content output from the personal computer 1-1.

[0170] Referring to FIG. 10, there is shown a process of registering the personal computers 1-1 through 1-3 which belong to the same group with the approval server 3.

[0171] When the first personal computer 1-1 belonging to the same group is registered with the approval server 3, the personal computer 1-1 transmits the user's credit card number, name, and mail address, for example, to the approval server 3, along with the ID of the content management program 51 of the personal computer 1-1. The approval server 3 records the received ID of the content management program 51, credit card number, name, and mail address to register the personal computer 1-1 and its user. When the registration has been completed, the approval server 3 transmits the group key 271 to the personal computer 1-1 along with the ID and password of the group. The personal computer 1-1 stores the group key 271 supplied from the approval server 3.

[0172] The ID of the group supplied by the approval server 3 is the user's credit card number. The password which is alternatively transmitted by the approval server 3 is the user's credit card number.

[0173] If the ID or password of a group is disclosed to a third party, the possibility that the users belonging to the group will suffer unexpected disadvantages increases. Therefore, the user of the personal computer 1-1 belonging to the group does not disclose the ID and password of the group to any third parties. This makes it practicable for the content output from the personal computer 1-1 to be used by a plurality of devices without being exposed to unauthorized usage.

[0174] When personal computer 1-2 belonging to the group to which the personal computer 1-1 belongs is registered with the approval server 3, the personal computer 1-2 transmits the ID and other information of the content management program 51 of the personal computer 1-2 to the approval server 3. The approval server 3 records the received ID and other information of the content management program 51 to register the personal computer 1-2. Then, the approval server 3 transmits the group key 271 to the personal computer 1-2. The personal computer 1-2 stores the received group key 271.

[0175] When the personal computer 1-3 belonging to the group to which the personal computer 1-1 belongs is registered with the approval server 3, the personal computer 1-3 transmits the ID and other information of the content management program 51 of the personal computer 1-3 to the approval server 3. The approval server 3 records the received ID and other information of the content management program 51 to register the personal computer 1-3. Then, the approval server 3 transmits the group key 271 to the personal computer 1-3. The personal computer 1-3 stores the received group key 271 from the approval server 3.

[0176] Thus, the personal computers 1-1 through 1-3 belonging to the same group store the same group key 271.

[0177] Referring to FIG. 11, there is shown a schematic diagram illustrating the import processing of content. When importing content from the personal computer 1-1, the personal computer 1-2 asks the user to input the ID and password of the group and the approval server 3 for an approval.

[0178] When the correct ID and password of the group have been input and an approval has come from the approval server 3,

the personal computer 1-2 executes the import of the content from the personal computer 1-1.

[0179] The following describes the registration process by the personal computer 1 which executes the group gateway program 61 and the approval server 3 with reference to the flowchart shown in FIG. 12.

[0180] In step S1101, the group gateway program 61 gets the credit card number input by the user at the keyboard 78, for example. In step S1102, the group gateway program 61 gets the ID from the content management program 51 and transmits this ID and the credit card number to the approval server 3 via the network 2.

[0181] In step S2101, the approval server 3 receives the ID of the content management program 51 and the credit card number from the personal computer 1. In step S2102, the approval server 3 determines on the basis of the received credit card number whether the personal computer 1 is the first one which belongs to the group. If the personal computer 1 is determined to be the first one, then the approval server 3 generates the group key 271 in step S2103. In step S2104, the approval server 3 generates the ID or password of the group which is the same as the credit card number.

[0182] In step S2105, the approval server 3 generates an account corresponding to the user, upon which the procedure goes to step S2106.

[0183] In step S2102, if the personal computer 1 is determined not to be the first one of the group, namely the second or subsequent one, then it is not necessary to generate the group key 271 and the account, upon which the procedure goes to step S2106, skipping steps S2103 through S2105.

[0184] In step S2106, the approval server 3 registers the ID of the content management program 51. In step S2107, the approval server 3 transmits the group key 271 and the group ID and password to the personal computer 1 via the network 2.

[0185] In step S1103, the group gateway program 61 receives the group key 271 and the group ID and password from the approval server 3. In step S1104, the group gateway program 61 records the group key 271 and the group ID and password. In step S1105, the group gateway program 61 displays the group ID

and password on the display 80, upon which the registration process comes to an end.

[0186] Thus, by transmitting the ID of the content management program 51 and the credit card number to the approval server 3, the personal computer 1-1 can get the group key 271 and the group ID and password. On the other hand, when registering the personal computer 1-1, the approval server 3 gets the ID of the content management program 51 and the credit card number and records the obtained ID of the content management program 51 and credit card number along with the generated group ID and password.

[0187] The following describes, with reference to the flowchart shown in FIG. 13, one example of the process for generating the group ID and password corresponding to the process of step S2104 shown in FIG. 12.

[0188] In step S11, the approval server 3 gets the received credit card number. In step S12, the approval server 3 generates the group ID and password. In the process of step S12, the generated group ID or password is the same as the credit card number.

[0189] In step S13, the approval server 3 records the credit card number and the group ID and password in a corresponding manner, upon which the group ID and password generation processing comes to an end.

[0190] Thus, because the group ID or password generated by the approval server 3 is the same as the credit card number, the group ID and password are protected against disclosure to any third parties.

[0191] The following describes the process of outputting content of the personal computer 1 with reference to the flowchart shown in FIG. 14.

[0192] In step S31, the content management program 51 reads content 251 and the content key 252 from the content database 53. The content 251 is encrypted by its content key. The content key 252 is encrypted by the storage key 253.

[0193] In step S32, the content management program 51 decrypts the content key 252 by the stored storage key 253. The content management program 51 supplies the content 251 encrypted by the content key and a plaintext content key to

the group gateway program 61.

[0194] In step S33, the group gateway program 61 encrypts the content key by the stored group key 271 to generate the content key 272.

[0195] In step S34, the group gateway program 61 outputs the content 251 encrypted by the content key and the content key 272 encrypted by the group key 271, upon which the processing comes to an end.

[0196] Thus, the personal computer 1 can output the content 251 encrypted by the content key and the content key 272 encrypted by the group key 271.

[0197] The following describes the process of importing the content 251 of the personal computer 1 with reference to the flowchart shown in FIG. 15. In step S1201, the group gateway program 61 gets the content 251 encrypted by its content key and the content key 272 encrypted by the group 271 via the network 2 or a storage medium such as the magneto-optical disk 93, for example. In step S1202, the group gateway program 61 gets the group ID and password in response to the user operation made at the keyboard 78, for example.

[0198] In step S1203, the group gateway program 61 determines on the basis of the stored group ID and password whether the group ID and password obtained in step S1202 are valid. If the group ID and password are determined to be valid, then the group gateway program 61 transmits the group ID and password to the approval server 3 via the network 2 in step S1204.

[0199] In step S2201, the approval server 3 receives the group ID and password from the personal computer 1. In step S2202, the approval server 3 determines on the basis of the recorded group ID and password whether the group ID and password received in step S2201 are valid. If the group ID and password are determined to be valid, then the approval server 3 transmits information for approving the personal computer 1 via the network 2 in step S2203.

[0200] In step S1205, the group gateway program 61 receives the approval information from the approval server 3. In step S1206, the group gateway program 61 decrypts the content key 272 by the group key 271. The group gateway program 61

supplies the decrypted content key to the content management program 51. In step S1207, the content management program 51 encrypts the content key by the storage key 253. In step S1208, the content management program 51 records the content 251 encrypted by the content key and the content key 252 encrypted by the storage key 253 in the content database 53, upon which the import process comes to an end.

[0201] If the group ID and password are determined to be invalid in step S1203, the import of the content 251 cannot be permitted, so that the import process comes to an end without recording the content 251 into the content database 53.

[0202] If the group ID and password are determined to be invalid in step S2202, the personal computer 1 cannot be approved, so that the process comes to an end without recording the content 251 into the content database 53.

[0203] Thus, the personal computer 1 imports the content 251 only when the correct ID and password have been input by the user and the personal computer 1 has been approved by the approval server 3.

[0204] Referring to FIG. 16, there is shown a schematic diagram illustrating another example of the management of the group ID and password.

[0205] In the registration process, the personal computer 1 transmits the fee-charging information, such as the credit card number, to the approval server 3. The approval server 3 transmits the received credit card number to the ID management server 8 and gets the group ID and password from the ID management server 8.

[0206] Receiving the credit card number from the approval server 3 for the first time, the ID management server 8 generates the group ID and password including the credit card number and stores the resultant group ID and password in correspondence with the credit card number, while transmitting the group ID and password to the approval server 3. The ID management server 8, if the credit card number received from the approval server 3 is already stored (for example, if the credit card number is already stored by the EMD server 4), transmits the ID and password stored in correspondence with the credit card number to the approval server 3 as the group

ID and password.

[0207] The approval server 3 transmits the group ID and password to the personal computer 1.

[0208] Receiving the credit card number from the EMD server 4 for the first time, the ID management server 8 generates the ID and password including the credit card number and stores the resultant group ID and password in correspondence with the credit card number, while transmitting the group ID and password to the EMD server 4. The ID management server 8, if the credit card number received from the EMD server 4 is already stored (for example, if the credit card number is already stored by the approval server 3), transmits the ID and password stored in correspondence with the credit card number to the EMD server 4.

[0209] The EMD server 4 transmits the ID and password to the personal computer 1.

[0210] Consequently, registration of the group ID and password with the approval server 3 and then with the EMD server 4 or vice versa causes the group ID and password to become the same as the ID and password registered with the EMD server 4.

[0211] Therefore, each user who knows the group ID and password can purchase content from the EMD server 4 only by entering the group ID and password. The EMD server 4 which sold content reads the credit card number from the ID management server 8 by referencing the input group ID and password and executes the fee-charging process for the content purchase.

[0212] If the ID or password of a group is disclosed to a third party, the possibility that the users belonging to the group will suffer unexpected disadvantages increases. Therefore, the user of the personal computer 1 belonging to the group does not disclose the ID and password of the group to any third parties. This makes it practicable for the content output from the personal computer 1 to be used by a plurality of devices without being exposed to unauthorized usage.

[0213] The following describes the registration process to be executed when the ID management server 8 generates the ID

and password with reference to the flowchart shown in FIG. 17.

[0214] In step S1301, the group gateway program 61 gets the credit card number input by the user at the keyboard 78, for example. In step S1302, the group gateway program 61 gets the ID from the content management program 51 and transmits the ID and the credit card to the approval server 3 via the network 2.

[0215] In step S2301, the approval server 3 receives the ID of the content management program 51 and the credit card number from the personal computer 1. In step S2302, the approval server 3 determines on the basis of the credit card number whether the personal computer 1 is the first one of the group. If the personal computer 1 is determined to be the first one, then the approval server 3 generates the group key 271 in step S2303. In step S2304, the approval server 3 transmits the credit card number to the ID management server 8 via the network 2.

[0216] In step S3301, the ID management server 8 receives the credit card number. In step S3302, the ID management server 8 executes the process of generating the ID and password. In step S3303, the ID management server 8 transmits the generated ID and password to the approval server 3 via the network 2.

[0217] In step S2305, the approval server 3 receives the ID and password. In step S2306, the approval server 3 generates the account for the user, upon which the procedure goes to step S2307.

[0218] In step S2302, if the personal computer 1 is determined not to be the first one of the group, namely the second or subsequent one, then it is not necessary to generate the group key 271 and the account, upon which the procedure goes to step S2307, skipping steps S2303 through S2306.

[0219] The process of each of steps S2307 through S1305 is the same as the process of each of steps S2106 through S1105, so that their descriptions will be skipped.

[0220] The following describes, with reference to the flowchart shown in FIG. 18, the process of generating ID and password by the ID management server 8 corresponding to the process of step S3302 shown in FIG. 17.

[0221] In step S51, the ID management server 8 determines

whether or not the credit card number received by the reception process has been registered. If the credit card number is determined to be not registered, then the ID management server 8 generates the ID and password in step S52. In the process of step S52, the generated ID or password is the same as the credit card number.

[0222] In step S53, the ID management server 8 records the credit card number and the ID and password in a corresponding manner, upon which the processing comes to an end.

[0223] If the credit card number is determined to be registered in step S51, then the ID management server 8 reads the ID and password which are recorded in correspondence with the credit card number in step S54, upon which the processing comes to an end.

[0224] The following describes the registration process to be executed by the personal computer 1 and the EMD server 4 with reference to the flowchart shown in FIG. 19. In step S1401, the personal computer 1 gets the credit card number in response to the operation performed by the user at the keyboard 78, for example. In step S1402, the personal computer 1 transmits the credit card number to the EMD server 4 via the network 2.

[0225] In step S2401, the EMD server 4 receives the credit card number from the personal computer 1. In step S2402, the EMD server 4 transmits the credit card number to the ID management server 8 via the network 2.

[0226] In step S3401, the ID management server 8 receives the credit card number from the EMD server 4. In step S3402, the ID management server 8 generates the ID and password. The details of the process of step S3402 are the same as the process described with reference to the flowchart shown in FIG. 18, so that their description will be skipped.

[0227] In step S3403, the ID management server 8 transmits the ID and password to the EMD server 4 via the network 2.

[0228] In step S2403, the EMD server 4 receives the ID and password. In step S2404, the EMD server 4 generates an account. In step S2405, the EMD server 4 transmits the ID and password to the personal computer 1 via the network 2.

[0229] In step S1403, the personal computer 1 receives the

ID and password. In step S1404, the personal computer 1 displays the received ID and password, upon which the processing comes to an end.

[0230] Thus, the group ID and password to be issued by the approval server 3 can be made the same as the ID and password to be issued by the EMD server 4.

[0231] The following describes the process of settlement to be executed when content has been purchased from the EMD server 4 with reference to the flowchart shown in FIG. 20. In step S1501, in response to the operation performed by the user at the keyboard 78, for example, the personal computer 1 gets the group ID and password or the ID and password registered with the EMD server 4. In step S1502, the personal computer 1 transmits a settlement request to the EMD server 4 along with the ID and password via the network 2.

[0232] In step S2501, the EMD server 4 receives the ID and password and the settlement request from the personal computer 1. In step S2502, the EMD server 4 transmits the ID and password to the ID management server 8 via the network 2.

[0233] In step S3501, the ID management server 8 receives the ID and password from the EMD server 4. In step S3502, the ID management server 8 reads the credit card number which corresponds to the received ID and password. In step S3503, the ID management server 8 transmits the retrieved credit card number to the EMD server 4 via the network 2.

[0234] In step S2503, the EMD server 4 receives the credit card number from the ID management server 8. In step S2504, the EMD server 4 executes a fee-charging process on the basis of the received credit card number, upon which the settlement process comes to an end.

[0235] Thus, the EMD server 4 can execute a fee-charging process by use of the group ID and password or the ID and password registered with the EMD server 4.

[0236] The following describes another process in which the personal computer 1 imports content with reference to FIG. 21.

[0237] In this example, when the registration has been made with the approval server 3, the group gateway program 61 of the personal computer 1 does not get the group key but gets only the group ID and password.

[0238] When the import of content 251 is requested and the group ID and password are entered by the user, the group gateway program 61 transmits the group ID and password to a decryption authentication server 331 via the network 2. Receiving the group ID and password from the personal computer 1, the decryption authentication server 331 transmits the group ID and password to the approval server 3.

[0239] Receiving the group ID and password from the decryption authentication server 331, the approval server 3 determines on the basis of the stored group ID and password whether the received group ID and password are valid. The approval server 3 transmits the result of this determination to the decryption authentication server 331.

[0240] If the group ID and password are determined to be valid, the decryption authentication server 331 generates the group key 271 on the basis of the group ID and password and transmits the generated group key 271 to the personal computer 1 via the network 2.

[0241] On the other hand, if the group ID and password are determined to be invalid, the decryption authentication server 331 ends the processing without generating the group key 271.

[0242] Thus, if the generation of the group key 271 is requested on the basis of the group ID and password which are invalid for some reason or other, the decryption authentication server 331 will not generate the group key 271.

[0243] Further, every time content is decrypted, the decryption authentication server 331 generates the group key 271, so that the decryption authentication server 331 can know the usage situation of the content.

[0244] As described, the group gateway program 61 does not hold the group key 271 and does not have a procedure for generating the group key 271, so that the personal computer 1 can more firmly prevent the unauthorized import of content.

[0245] The following describes the process of transmission of the group key 271 to be executed by the decryption authentication server 331 with reference to the flowchart shown in FIG. 22. In step S71, the decryption authentication server 331 receives the group ID and password from the personal computer 1 via the network 2. In step S72, the

decryption authentication server 331 transmits the group ID and password to the approval server 3 to ask if the group ID and the password are valid. The approval server 3 transmits the information telling whether the group ID and password are valid to the decryption authentication server 331.

[0246] In step S73, the decryption authentication server 331 determines on the basis of the information received from the approval server 3 whether the group ID and password are valid. If the group ID and password are determined to be valid, the decryption authentication server 331 generates the group key 271 on the basis of the group ID and password in step S74. In step S75, the decryption authentication server 331 transmits the generated group key 271 to the personal computer 1 via the network 2, upon which the processing comes to an end.

[0247] If the group ID and password are determined to be invalid in step S73, it indicates that the import cannot be permitted, so that the decryption authentication server 331 ends the processing without transmitting the group key 271 to the personal computer 1.

[0248] Thus, if the group ID and password received from the personal computer 1 are determined to be valid, the decryption authentication server 331 generates the group key 271 and transmits it to the personal computer 1; if the group ID and password are determined to be invalid, the decryption authentication server 331 does not generate the group key 271. Consequently, the personal computer 1 can import the content 251 only when the good group ID and password have been entered.

[0249] The following describes an operation of the locker server 11.

[0250] Referring to FIG. 23, there is shown a schematic diagram illustrating registration with the locker server 11. The locker server 11 is connected to a content database 401 and a log database 402.

[0251] The locker server 11 records content supplied from the personal computer 1 in the content database 401.

[0252] The content database 401 records the content received by the locker server 11 from the registered personal computer 1 and supplies the recorded content to the locker server 11 when requested thereby.

[0253] The locker server 11 transmits the content supplied from the content database 401 to the personal computer 1 via the network 2.

[0254] The log database 402 records a log of the registration of the personal computer 1 with the locker server 11 and the recording and retrieval of content.

[0255] When requesting the registration of the personal computer 1 with the locker server 11, the personal computer 1 transmits the credit card number to the locker server 11.

[0256] The locker server 11 generates an ID and records the generated ID in the log database 402 and, at the same time, transmits the generated ID to the personal computer 1. The ID generated by the locker server 11 is the same as the credit card number of the user of the personal computer 1, for example.

[0257] The locker server 11 transmits a log indicative of the registration of the personal computer 1 to the personal computer 1 and executes the process of fee-charging for the registration, transmitting a result thereof to the personal computer 1.

[0258] Referring to FIG. 24, there is shown a diagram illustrating a list of content items recorded in the locker server 11. As shown, the locker server 11 records the content names in association with the IDs of the registered users.

[0259] For example, the locker server 11 records content name "AAAAA" in correspondence with user ID "aaaaa," content name "BBBBB" in correspondence with user ID "bbbbb," and content name "CCCCC" in correspondence with user ID "ccccc."

[0260] Referring to FIG. 25, there is shown a schematic diagram illustrating a content sharing operation by the locker server 11. The locker server 11 records the content supplied from the personal computer 1-1 in the content database 401. Then, the locker server 11 records the name of the content in the content list in correspondence with the ID of the user of the personal computer 1-1 and stores, in the log database 402, a log indicative of the recording of the content in the content database 401.

[0261] When the transmission of the content is requested from the personal computer 1-2 on the basis of the same ID as

the personal computer 1-1, the locker server 11 determines on the basis of the content list whether the user ID is valid. If the user ID is determined to be valid, the locker server 11 asks the content database 401 to supply the content. The locker server 11 transmits the content supplied from the content database 401 to the personal computer 1-2. Then, the locker server 11 stores, in the log database 402, a log indicative of the supply of the content to the personal computer 1-2.

[0262] As shown in FIG. 26, the personal computer 1-1 can also transmit the content purchased from the EMD server 4 to the locker server 11 to record the content in the content database 401. In this case, too, when the transmission of the content is requested by the personal computer 1-2, the locker server 11 asks, on the basis of the same ID as that of the personal computer 1-1, the content database 401 to supply the content and transmits the supplied content to the personal computer 1-2.

[0263] As shown in FIG. 27, the locker server 11 may transmit a log indicative of the registration of the personal computer 1 to the personal computer 1 and, by executing monthly fee-charging for the registration, transmit a result of this execution to the personal computer 1.

[0264] The following describes registration processing by the personal computer 1 and the locker server 11 with reference to the flowchart shown in FIG. 28.

[0265] In step S1601, the personal computer 1 gets the credit card number input by the user at the keyboard 78, for example. In step S1602, the personal computer 1 transmits the credit card number to the locker server 11 via the network 2.

[0266] In step S2601, the locker server 11 receives the credit card number from the personal computer 1. In step S2602, the locker server 11 determines on the basis of the received credit card number whether the registration has been made for the first time. If the registration is determined to be made for the first time, the locker server 11 generates the user ID in step S2603. In step S2604, the locker server 11 records the generated user ID, upon which the procedure goes to step S2605.

[0267] If the registration is determined not to be made for

the first time in step S2602, the user ID need not be generated, so that the procedure goes to step S2605, skipping steps S2603 and S2604.

[0268] In step S2605, the locker server 11 records a log indicative of the registration of the user ID with the log data base 402. In step S2606, the locker server 11 transmits the user ID and the log to the personal computer 1 via the network 2.

[0269] In step S1603, the personal computer 1 receives the user ID and the log transmitted from the locker server 11. In step S1604, the personal computer 1 records the received user ID and log. In step S2607, the locker server 11 determines on the basis of the received credit card number whether the registration has been made for the first time. If the registration is determined to be made for the first time, the locker server 11 executes a fee-charging process on the basis of the received credit card number in step S2608, upon which the processing comes to an end.

[0270] If the registration is determined not to be made for the first time in step S2607, a fee-charging process is not required, so that step S2608 is skipped, upon which the processing comes to an end.

[0271] Thus, by transmitting the credit card number to the locker server 11, the personal computer 1 can get the user ID. On the other hand, when registering the personal computer 1, the locker server 11 can get the credit card number and record it along with the generated user ID.

[0272] The following describes the process of recording content to the locker server 11 with reference to the flowchart shown in FIG. 29. In step S1701, the personal computer 1 transmits the content to the locker server 11 along with the user ID via the network 2.

[0273] In step S2701, the locker server 11 receives the content and the user ID transmitted from the personal computer 1. In step S2702, the locker server 11 determines on the basis of the user ID recorded in the list whether the received user ID has been registered. If the received user ID is determined to be registered, then the locker server 11 records the received content in the content database 401 in step S2703.

[0274] In step S2704, the locker server 11 records the log indicative of the recording of the content in the log database 402. In step S2705, the locker server 11 transmits the log indicative of the recording of the content to the personal computer 1 via the network 2.

[0275] In step S1702, the personal computer 1 receives the log indicative of the recording of the content from the locker server 11. In step S1703, the personal computer 1 records the received log. In step S1704, the personal computer 1 displays the received log on the display 80, upon which the processing comes to an end.

[0276] If the received user ID is determined not to be registered in step S2702, it indicates that the request for recording the content is unauthorized, so that the processing comes to an end without recording the content.

[0277] Thus, upon reception of the content with a valid ID, the locker server 11 stores the received content in the content database 401; upon reception of the content with an invalid ID, the locker server 11 discards the received content.

[0278] The following describes the retrieval of content from the locker server 11 with reference to the flowchart shown in FIG. 30. In step S1801, the personal computer 1 transmits a request for content to the locker server 11 along with the user ID via the network 2.

[0279] In step S2801, the locker server 11 receives the content request and the user ID transmitted from the personal computer 1. In step S2802, the locker server 11 determines on the basis of the recorded user ID whether the received user ID has been registered. If the received user ID is determined to be recorded, the locker server 11 reads the requested content from the content database 401 in step S2803.

[0280] In step S2804, the locker server 11 records a log indicative of the content retrieval in the log database 402. In step S2805, the locker server 11 transmits the retrieved content and the log indicative of the retrieval of the content to the personal computer 1 via the network 2.

[0281] In step S1802, the personal computer 1 receives the content and log transmitted from the locker server 11. In step S1803, the personal computer 1 records the received content

and log. In step S1804, the personal computer 1 displays the received log on the display 80, upon which the processing comes to an end.

[0282] If the received user ID is determined not to be registered in step S2802, it indicates that the content request is unauthorized, so that the processing comes to an end without transmitting the content.

[0283] Thus, upon reception of the registered user ID and the request for content, the locker server 11 retrieves the requested content from the content database 401 and transmits the retrieved content; if the user ID has not been registered, the locker server 11 will not transmit the content.

[0284] The following describes a music data management system practiced as a second embodiment of the invention.

[0285] Referring to FIG. 31, there is shown the second embodiment of the invention. As shown, a public switched line network 503 is connected to PDAs 501-1 and 501-2 and camera-mounted digital mobile telephones 16-1 and 16-2 via base stations 502-1 through 502-4, which are stationary wireless stations each arranged in each of the cells obtained by dividing a communication service area by a certain factor.

[0286] The base stations 502-1 through 502-4 are connected to the PDAs 501-1 and 501-2, which are mobile wireless stations, and the camera-mounted digital mobile telephones 16-1 and 16-2 in a wireless manner based on W-CDMA (Wideband Code Division Multiple Access), for example, to transfer mass data at speeds up to 2 Mbps by use of a 2-GHz frequency band.

[0287] The PDAs 501-1 and 501-2 and the camera-mounted digital mobile telephones 16-1 and 16-2 can transfer mass data at high speeds with the base stations 502-1 through 502-4, so that not only voice but also electronic mail transfer, simplified home page browsing, transfer of content-like images, and other various kinds of data communications can be executed.

[0288] The PDAs 501-1 and 501-2 and the camera-mounted digital mobile telephones 16-1 and 16-2 execute browser programs, the content management program 51, and group gateway program 61 to execute content management and content input/output processing.

[0289] The base stations 502-1 through 502-4 are connected

to the public switched line network 503 with cables. The public switched line network 503 is connected to the Internet, the network 2, subscriber-wired terminal devices, not shown, a computer network, not shown, and a local area network, not shown, for example.

[0290] An access server 504 of an Internet service provider is connected to the public switched line network 503 and to a content server 505 owned by the Internet service provider.

[0291] In response to a request from a subscriber-wired terminal device, the PDA 501-1 or 501-2, or the camera-mounted digital mobile telephone 16-1 or 16-2, the content server 505 provides content, such as a simplified home page, for example, as a compact HTML (Hyper Text Markup Language) file.

[0292] The network 2 is connected to many WWW (World Wide Web) servers 506-1 through 506-N. The WWW servers 506-1 through 506-N are accessed from the subscriber wired terminal devices, the PDAs 501-1 and 501-2, and the camera-mounted digital mobile telephones 16-1 and 16-2 in accordance with TCP (Transmission Control Protocol/IP (Internet Protocol)).

[0293] The WWW servers 506-1 through 506-N execute generally the same processing as the approval server 3, the EMD server 4, the ID management server 8, and the locker server 11 to provide content, for example, to the PDAs 501-1 and 501-2 or the camera-mounted digital mobile telephones 16-1 and 16-2 via the network 2, record content, transmit content, and manage IDs.

[0294] The PDAs 501-1 and 501-2 and the camera-mounted digital mobile telephones 16-1 and 16-2 communicate with the base stations 502-1 through 502-4 by means of a simplified transport protocol of 2 Mbps and communicate between the base stations 502-1 through 502-4 and the network 2 and the WWW servers 506-1 through 506-N by means of TCP/IP.

[0295] It should be noted that a management control apparatus 507 is connected to the subscriber-wired terminal devices, the PDAs 501-1 and 501-2, and the camera-mounted digital mobile telephones 16-1 and 16-2 via the public switched line network 503, executing the authentication process and fee-charging process for the subscriber-wired terminal devices, the PDAs 501-1 and 501-2, and the camera-

mounted digital mobile telephones 16-1 and 16-2.

[0296] The camera-mounted digital mobile telephones 16-1 and 16-2 use content by generally the same process as the personal computer 1 via the public switched line network 503 and the network 2.

[0297] In what follows, the camera-mounted digital mobile telephones 16-1 and 16-2 will be generically referred to simply as a camera-mounted digital mobile telephone 16 unless otherwise noted.

[0298] The following describes the external configuration of the camera-mounted digital mobile telephone 16 to which the present invention is applied. As shown in FIG. 32, the camera-mounted digital mobile telephone 16 is composed of a display section 531 and a main body 532 which are pivotally connected with a hinge 533 in between.

[0299] The display section 531 has a retractable send/receive antenna 534 at its upper left corner. The digital mobile telephone 16 transmits and receives signals to and from the base stations 502-1 through 502-4, which are stationary wireless terminals, via the antenna 534.

[0300] The display section 531 has, on its top center, a camera section 535 which is pivotable within an angular range of about 180 degrees. The camera-mounted digital mobile telephone 16 takes pictures by a CCD camera 536 incorporated in the camera section 535.

[0301] When the camera section 535 is rotated by the user about 180 degrees, the display section 531 is positioned with a speaker 537 arranged at the rear center of the camera section 535 faced to the front side, as shown in FIG. 33. Thus, the camera-mounted digital mobile telephone 16 can be configured in the normal talk mode.

[0302] In addition, the display section 531 has a liquid crystal display 538 at the front center section. The liquid crystal display 538 displays the contents of electronic mail, a simplified home page, and an image taken by the CCD camera 536 of the camera section 535 in addition to radio wave reception status, battery remaining amount, and names and telephone numbers and a call log registered as a telephone directory.

[0303] On the other hand, the main body 532 has numeric keys "0" through "9", a call key, a redial key, a clear/power key, and other operator keys 539 on the front surface. Various commands are input from these operator keys 539 into the camera-mounted digital mobile telephone 16.

[0304] Below the operator keys 539 of the main body 532, a memo button 540 and a microphone 541 are arranged. When the memo button 540 is pressed, the camera-mounted digital mobile telephone 16 records the voice of the other party. The camera-mounted digital mobile telephone 16 picks up the voice of the user in the talk mode through the microphone 541.

[0305] In addition, a rotatable jog dial 542 is arranged over the operator keys 539 on the main body 532 in a manner in which the jog dial 542 is slightly projecting from the surface of the main body 532. In accordance with the rotary operation of the jog dial 542, the camera-mounted digital mobile telephone 16 executes the scrolling of a telephone directory list or electronic mail messages displayed on the liquid crystal display 538, the turning of the displayed pages of a simplified home page, and the feeding of displayed images, for example.

[0306] For example, the main body 532 selects a desired telephone number from among those in a telephone directory list displayed on the liquid crystal display 538 by the rotation of the jog dial 542 by the user and, when the jog dial 542 is pressed into the main body 532, enters the selected telephone number, thereby automatically originating a call to the party at the selected telephone number.

[0307] It should be noted that a battery pack, not shown, is loaded in the main body 532 at the rear side. When the clear/power key is turned on, power is supplied from the battery pack to each circuit, making the camera-mounted digital mobile telephone 16 ready for operation.

[0308] The main body 532 also has a Memory Stick (trademark) slot 543 at the upper left side in which the detachable memory card 13 is loaded. When the memo button 540 is pressed, the camera-mounted digital mobile telephone 16 records the voice of the other party onto the loaded memory card 13. In accordance with the operation of the user, the

camera-mounted digital mobile telephone 16 records an electronic mail message, a simplified home page, or an image taken by the CCD camera 536 onto the loaded memory card 13.

[0309] The memory card 13 is a Memory Stick (trademark), for example. The Memory Stick is a kind of flash memory card developed by Sony Corporation, the applicant hereof. The memory card 13 incorporates a flash memory element, one kind of EEPROM (Electrically Erasable and Programmable Read Only Memory), housed in a plastic case having dimensions of 21.5mm × 50mm × 2.8mm. The memory card 13 allows writing and reading of various data such as images, voices, and music via a 10-pin terminal.

[0310] The Memory Stick uses a proprietary serial protocol which guarantees compatibility with the devices in which it is used even if the specifications of the incorporated flash memory have been changed due to the increase in its capacity, for example, realizes the high-speed performance of maximum write rate of 1.5 MB/S and maximum read rate of 2.45 MB/S, and ensures high reliability by the provision of an error deletion preventing switch.

[0311] Consequently, the camera-mounted digital mobile telephone 16, configured to detachably load the memory card 13, can share data with other electronic devices via the memory card 13.

[0312] As shown in FIG. 34, the camera-mounted digital mobile telephone 16 is configured so that a main controller 551 for centrally controlling each portion of the display section 531 and the main body 532 is connected to a power supply circuit 552, an operation input controller 553, an image encoder 554, a camera interface section 555, an LCD (Liquid Crystal Display) controller 556, an image decoder 557, a multiplexer/demultiplexer 558, a recording/reproducing section 563, a modulator/demodulator 559, and an audio codec 560 via a main bus 561. The image encoder 557, the image decoder 557, the multiplexer/demultiplexer 558, and the audio codec 560 are interconnected by a synchronous bus 562.

[0313] The power supply circuit 552, when the clear/power key is turned on by the user, supplies power from the battery pack to each component circuit, thereby making the camera-

mounted digital mobile telephone 16 ready for operation.

[0314] Under the control of the main controller 551 composed of a CPU, a ROM, and a RAM for example, the camera-mounted digital mobile telephone 16 converts an audio signal picked up by the microphone 541 in the talk mode into digital audio data through the audio codec 560. The camera-mounted digital mobile telephone 16 performs spread spectrum on the digital audio data through a modulator/demodulator 559 and performs digital-to-analog conversion and then frequency conversion on the digital audio data through a send/receive circuit 564, sending the resultant digital audio data via the antenna 534.

[0315] The camera-mounted digital mobile telephone 16 amplifies a signal received at the antenna 534 in the talk mode, performs frequency conversion and analog-to-digital conversion on the amplified signal, performs spread spectrum on the converted signal through the modulator/demodulator 559, and converts the resultant signal into an analog audio signal through the audio codec 560. The camera-mounted digital mobile telephone 16 outputs a sound corresponding to this analog audio signal from the speaker 537.

[0316] Further, in the data communication mode, when sending content, the camera-mounted digital mobile telephone 16 sends the specified content input from the operator keys 539 and the jog dial 542 to the main controller 551.

[0317] The main controller 551 performs spread spectrum on the text data through the modulator/demodulator 559 and then digital-to-analog conversion and frequency conversion through the send/receive circuit 564, sending the resultant text data to the base station via the antenna 534.

[0318] In the data communication mode, when receiving content, the camera-mounted digital mobile telephone 16 performs reverse spread spectrum, through the modulator/demodulator 559, on the signal received from the base station via the antenna 534 to restore the original content and displays the original content on the liquid crystal display 538 through the LCD controller 556.

[0319] The LCD controller 556, like the locker server 11, is connected to the liquid crystal display 538 via a flexible

printed circuit board having a panel ID setting section.

[0320] Then, the camera-mounted digital mobile telephone 16 can also record the content received in response to user operation onto the memory card 13 via the recording/reproducing section 563.

[0321] In the data communication mode, when sending image data, the camera-mounted digital mobile telephone 16 supplies the image data taken by the CCD camera 536 to the image encoder 554 via the camera interface section 555.

[0322] When not sending image data, the camera-mounted digital mobile telephone 16 can also display the image data taken by the CCD camera 536 on the liquid crystal display 538 via the camera interface section 555 and the LCD controller 556.

[0323] The image encoder 554 converts the image data supplied from the CCD camera 536 into coded image data by coding and compressing based on MPEG2 (Motion Picture Experts Group 2) or MPEG4, for example, and sends the coded image data to the multiplexer/demultiplexer 558.

[0324] At this moment, the camera-mounted digital mobile telephone 16 sends an audio signal picked up by the microphone 541 while taking the image by the CCD camera 536 to the multiplexer/demultiplexer 558 via the audio codec 560 as digital audio data.

[0325] The multiplexer/demultiplexer 558 multiplexes the coded image data supplied from the image encoder 554 with the audio data supplied from the audio codec 560 by a predetermined algorithm, performs spread spectrum on the resultant multiplexed data through the modulator/demodulator 559, and performs digital-to-analog conversion and frequency conversion through the send/receive circuit 564, outputting the resultant data via the antenna 534.

[0326] In the data communication mode, when receiving the data of a moving image file linked with a simplified home page, for example, the camera-mounted digital mobile telephone 16 performs reverse spread spectrum on the signal received from the base station via the antenna 534 through the modulator/demodulator 559 and sends the resultant multiplexed data to the multiplexer/demultiplexer 558.

[0327] The multiplexer/demultiplexer 558 divides the multiplexed data into coded image data and audio data, supplying the coded image data to the image decoder 557 and the audio data to the audio codec 560 via a synchronous bus 562.

[0328] The image decoder 557 generates reproduced moving image data by decoding the coded image data by the corresponding predetermined decoding algorithm such as MPEG2 or MPEG4, for example, and supplies the reproduced moving image data to the liquid crystal display 538 via the LCD controller 556. Consequently, the camera-mounted digital mobile telephone 16 displays the moving image data contained in a moving image file linked with a simplified home page, for example.

[0329] At the same time, the audio codec 560 converts the audio data into an analog audio signal and supplies it to the speaker 537. Consequently, the camera-mounted digital mobile telephone 16 reproduces the audio data contained in the moving image file linked with the simplified home page, for example.

[0330] It should be noted that, in the above-mentioned examples, the personal computer 1 or the camera-mounted digital mobile telephone 16 has been described to transmit the credit card number and the approval server 3, the ID management server 8, or the locker server 11 has been described to record the received credit card number; however, instead of the credit card number, the user's bank account number, Internet service provider registration number, or any other information which is available for fee-charging processing may be used.

[0331] The above-mentioned sequences of processes may be executed by hardware but they may also be executed by software. The execution by software is supported by a computer in which the programs constituting this software are stored in a dedicated hardware storage device or a general-purpose personal computer, for example, in which these programs are installed from a program storage medium.

[0332] The program storage medium storing the programs which are installed in a general-purpose personal computer, for example, to be made executable by the computer is a

package medium constituted by the magnetic disk 91 or 131 (including floppy disk), the optical disk 92 or 132 (including CD-ROM (Compact Disk Read Only Memory) and DVD (Digital Versatile Disk)), the magneto-optical disk 93 or 133 (including MD (Mini Disk)), or the semiconductor memory 94 or 134, as shown in FIG. 3 or 4, or the program storage medium is constituted by the ROM 72 or 102, or the HDD 81 or 111, for example, which store the programs on a temporary or permanent basis. As required, the programs are stored in the program storage medium by use of a wired or wireless communications medium such as a local area network, the Internet, or digital satellite broadcasting via such interface as a router or modem. The steps describing the programs provided by the above-mentioned program storage medium include not only processes which are executed in the described sequence in a time-dependent manner, but also processes which are executed in parallel or discretely.

[0333] It should be noted that term "system" herein denotes an entire apparatus constituted by a plurality of devices.

[0334] Although the invention herein has been described with reference to particular embodiments, it is to be understood that these embodiments are merely illustrative of the principles and applications of the present invention. It is therefore to be understood that numerous modifications may be made to the illustrative embodiments and that other arrangements may be devised without departing from the spirit and scope of the present invention as defined by the appended claims.